REMARKS

Reconsideration and allowance of the subject application are respectfully requested.

The undersigned wishes to thank the Examiner and his Supervisor for their time and cooperation during the personal interview of February 10, 2004. During the interview, the Examiner agreed that the prior art of record does not disclose a proxy encoding scheme in which the transformation key does not reveal the grantor's key. Further, the Examiner agreed that the prior art of record does not disclose that a transformation key can be generated based on ciphertext of the encrypted document, or a random variable. The use of the random variable and/or the ciphertext for creating the transformation key permits the transformation key to be used to decrypt the document while masking the grantor's key.

Claims 1-7 were pending prior to the Office Action of September 12, 2003. Claims 1 and 4 are currently amended herein. Support for the amendments to claims 1 and 4 can be found throughout the specification, more specifically, on page 20, lines 8-21 and 24-26, page 21, lines 4-6, page 30, lines 22-24, and page 32, lines 4-10. Dependent claims 8-13 have been added. Accordingly, claims 1-13 are pending in the present application.

Independent claims 1 and 4 recite that the grantor and grantee keys are used to generate a transformation key which is used to transform the document. The grantee's decryption key is then used to decrypt the file. Further, these claims expressly recite that the transformation key does not allow the grantee to determine the grantor's decryption key. In this manner, a system and method has been devised in which, unlike the prior art, the grantor need not trust the grantee. This permits a proxy encryption scheme in which the grantor can transfer the ability to decrypt a file to a grantee without the need for trust between the grantor and grantee, i.e. the grantee cannot ascertain the grantor's decryption key for the transfer key. This is described in the specification beginning on page 30, at line 16 and continuing through page 32, at line 10. In the specification, the grantor is party A and the grantee is party B. See page 26, lines 19-26. The prior art fails to disclose such a proxy encryption scheme and in fact teaches away from such a scheme.

For example, Schneier does not suggest the claimed double encryption and transformation which permits the grantee's decryption key to be used for decryption without

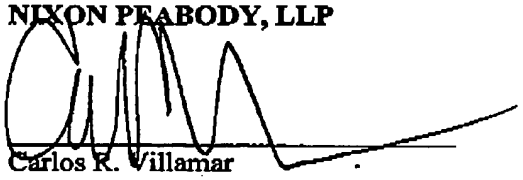
permitting the grantee to discover the grantor's decryption key. Instead, Schneier teaches to re-encrypt data with an encryption key, and that the encryption keys should expire periodically like passports and licenses. (Schneier, page 183) Similarly, Schneier teaches that, depending on the value of the data and the amount of data encrypted during a given period, keys could be replaced as frequently as once a day, assuming there is an efficient method of transferring new keys. (Schneier, page 184) Inherent in a decryption and a re-encryption is the possibility of exposure of the original data file. This exposure is prevented by the claimed invention by providing a transformation key which updates the encrypted data file into an updated encrypted data file equivalent to an encrypted data file encrypted with the grantee's key, without decrypting the encrypted data file during the encryption cycle.

Claims 8-13 depend from one of claims 1 and 4 and recite the novel features of generating the transformation key based on ciphertext and or a random variable. As noted by the Examiner during the interview, the prior art does not disclose these features.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. However, if the Examiner deems that any issue remains after considering this response, he is invited to call the undersigned to expedite the prosecution and work out any such issue by telephone.

Respectfully submitted,

NIXON PEABODY, LLP



Carlos R. Villamar
Registration No. 43,224

Date: **March 29, 2004**

Customer No.: 22204
NIXON PEABODY LLP
401 9th Street, NW, Suite 900
Washington, DC 20004
(202) 585-8000
(202) 585-8080 – FAX

MSK:kla
NVA289026.1